

Eduard Benderskiy: Western authorities link Russian intelligence officer to Evil Corp cybercrime empire

R therecord.media/evil-corp-cybercrime-eduard-benderskiy-russian-intelligence



Eduard Benderskiy in a hunting video uploaded to YouTube.

Alexander Martin

October 1st, 2024

Eduard Benderskiy, a former high-ranking official within the Russian intelligence services, was named and sanctioned by Western authorities on Tuesday in a move describing him as a key enabler and protector for the Evil Corp cybercrime group.

The identification of Benderskiy is the most significant publicly known link between the Russian state and the country's enormous and lucrative cybercrime underworld, although Western officials say the case is exceptional rather than the norm.

Evil Corp is an organized crime group that was sanctioned and indicted by the U.S. back in 2019. The gang has perpetrated numerous criminal campaigns over the past decade including the GameOverZeus and Dridex banking trojans and botnets. It is believed to have stolen hundreds of millions of dollars from victims worldwide.

At the time of the 2019 indictment, its leader Maksim Yakubets was also charged with providing direct assistance to the Russian government by using his access to victims' computers to acquire "confidential documents" for the FSB, Russia's internal security service, at the same time as conducting criminal activities.

Also named in the indictment were several of Yakubets' relatives, including his brother Artem Yakubets and his cousins Kirill and Dimitriy Slobodskoy. The leaders of the group, which investigators say formed more of a traditional vertical hierarchy than other Russian cybercrime groups, are known to socialize together, including with their families.



*Left to right: Kirill Slobodskoy, Maksim Yakubets, Dimitriy Slobodskoy and Artem Yakubets.
Image: NCA*

In the paper published Tuesday by the United Kingdom's National Crime Agency, the FBI and Australian Federal Police, Benderskiy was confirmed to be Yakubets' father-in-law and described as using his "extensive influence with the Russian state to protect the group," particularly following the sanctions and indictment.

The paper was published as the law enforcement agencies named another member of the Evil Corp group, Aleksandr Ryzhenkov, for the first time. Ryzhenkov is described as Yakubets' right-hand man, and is the most senior member of Evil Corp not directly related to Yakubets.

Read More: [Police unmask Aleksandr Ryzhenkov as Evil Corp member and LockBit affiliate](#)

In addition to his Evil Corp work, Ryzhenkov was identified as a LockBit affiliate by the NCA as it announced another tranche of information gleaned from LockBit's systems. Alongside Ryzhenkov and Benderskiy, the British government announced it was sanctioning a tranche of other Evil Corp members on Tuesday, and the U.S. Department of Justice unsealed an indictment charging Ryzhenkov for using BitPaymer ransomware to target victims across the U.S.

The U.S. Treasury also designated seven individuals and two entities associated with Evil Corp as part of the coordinated action, while the British government added 15 individuals to its cyber sanctions list, and the Australian government added three.

"Today's trilateral action underscores our collective commitment to safeguard against cybercriminals like ransomware actors, who seek to undermine our critical infrastructure and threaten our citizens," said the U.S. Treasury's Bradley Smith.

Benderskiy and Evil Corp

Prior to the indictment, Benderskiy was described as being a key enabler of the group's relationships with Russia's intelligence services, and in the wake of several of the group's senior members being outed, Benderskiy provided them with security and ensured they were not pursued by Russia's internal authorities.

Links between the Russian state and the cybercrime underworld are a regular concern for Western observers. Formally, the FSB is not empowered to investigate crimes committed in foreign territories and the Russian constitution forbids the extradition of Russian citizens.

While this has been described as the country's "tacit support" for cybercriminals, there are several cases that indicate a more engaged relationship between the security services and the cybercrime ecosystem, even "beyond the typical state-criminal relationship of protection, payoffs and racketeering."

Back in 2017 the U.S. charged two FSB officers for directing criminal hackers to compromise Yahoo accounts, while just last year the British and U.S. governments sanctioned cybercriminal Vitaly Kovalev, a senior member in the Trickbot group, who was described as having a relationship with the Russian intelligence services.

In the paper on Tuesday, Evil Corp was described as being tasked "to conduct cyberattacks and espionage operations against NATO allies" courtesy of Benderskiy's ongoing relationship with the Kremlin, although he does not appear to currently hold any formal position within the country's security apparatus.

Russian media has described Benderskiy as a veteran of the KGB's Vypmel group — now succeeded by the FSB's "Directorate V" — for which he appeared as a spokesperson in 2011, describing it as an elite unit working in "mountainous, hard-to-reach forested areas."

Benderskiy remains an active trophy hunter, appearing on numerous hunting websites and videos online, and is currently the president and chairman of the Club of Mountain Hunters (KGO-Club) in Russia.

A biography on the club's website describes him as a former member of the KGB special forces, and states he has operated both a security company and a charity using the Vypmel name.

As profiled by the investigative journalists at Bellingcat in 2020, Benderskiy was reported to have used the Vypmel charity to assist the FSB in assassinating Zelimkhan Khangoshvili, the Chechen former platoon commander, in a park in Berlin in 2019.

"Evidently, [Benderskiy] is a highly connected individual still closely involved with the Kremlin's activities," stated the NCA, FBI and AFP.

- Cybercrime
- Nation-state
- News
- People

Get more insights with the
Recorded Future

Intelligence Cloud.

Learn more.

Tags

- Russia
- Evil Corp
- intelligence agency
- LockBit
- United States
- United Kingdom
- Australia
- National Crime Agency (NCA)
- FBI
- Australian Federal Police
- sanctions
- BitPaymer
- FSB

- Indictment

No previous article

No new articles



Alexander Martin

is the UK Editor for Recorded Future News. He was previously a technology reporter for Sky News and is also a fellow at the European Cyber Conflict Research Initiative.